14

Uploading CPTPP and USMCA Provisions to the WTO's Digital Trade Negotiations Poses Challenges for National Data Regulation

Example from Canada

*Patrick Leblond**

A INTRODUCTION

Policymakers face a tension between, on the one hand, generating the economic benefits associated with unfettered data flows across borders and, on the other hand, providing a trusting environment for individuals, firms and governments taking part in the data-driven economy. International trade agreements seek to regulate data flows through provisions aiming to facilitate the cross-border trade of goods and services built on data, such as data processing and other computing services.[1]

On the margins of the G20 leaders' meeting in Osaka in June 2019, twenty-three countries plus the European Union (EU) signed the Osaka Declaration on the Digital Economy.[2] The declaration states that the signatories, 'standing together with other World Trade Organization (WTO) Members that participate in the Joint Statement on Electronic Commerce issued in Davos on 25 January 2019, in which 78 WTO Members are on board, hereby declare the launch of the "Osaka Track", a process which demonstrates our commitment to promote international policy discussions'. The referred-to January 2019 Joint Statement, issued during the World Economic Forum's annual meeting in Davos, confirms the members' 'intention to commence WTO negotiations on trade-related aspects of electronic commerce'.[3] This Joint Statement is itself a restatement of a previous Joint Statement issued at the

* Patrick Leblond is Associate Professor and CN-Paul M. Tellier Chair on Business and Public Policy in the Graduate School of Public and International Affairs at the University of Ottawa. He is also Senior Fellow at the Centre for International Governance Innovation (CIGI), Research Associate at CIRANO and Affiliated Professor of International Business at HEC Montréal. Contact: patrick.leblond@uottawa.ca.

[1] S. A. Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', *World Trade Review* 18 (2019), 541–577; M. Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation', *UC Davis Law Review* 51 (2017), 65–132.

[2] See www.wto.org/english/news_e/news19_e/osaka_declration_on_digital_economy_e.pdf.

[3] See WTO, Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

WTO's eleventh ministerial conference in Buenos Aires in December 2017, where some seventy-five members 'recognize[d] the important role of the WTO in promoting open, transparent, non-discriminatory and predictable regulatory environments in facilitating electronic commerce'.[4] The Buenos Aires Joint Statement indicated that the signatories would begin exploratory work toward 'future WTO negotiations on trade-related aspects of electronic commerce'.[5]

A number of discussion rounds took place in 2018 and 2019 in Geneva in order to delimit the scope of potential plurilateral negotiations on electronic commerce/digital trade. The provisions on e-commerce/digital trade found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[6] and the United States–Mexico–Canada Agreement (USMCA),[7] the North American Free Trade Agreement's (NAFTA) replacement, are currently the most detailed proposals being considered in the WTO's plurilateral negotiations on e-commerce.[8]

This is why this chapter offers a detailed analysis of these CPTPP/USMCA e-commerce/digital trade provisions that pertain to data flows in order to identify the constraints they could impose on national data regulation.[9] To do so, it uses Canada as an example, because it is a party to both trade agreements and it seeks to build a high-trust data environment for consumers and businesses.[10] The analysis leads to the conclusion that Canada's CPTPP and USMCA commitments could ultimately negate the effectiveness of future data protection policies that the Canadian federal government might want to adopt to achieve its 'trust in the digital age' objective.[11]

B CROSS-BORDER DATA FLOW AND NATIONAL DATA REGULATION

Policymakers have lots of reasons to try to link the free flow of data and data protection. According to Dan Ciuriak, 'there is a need for free flow of data,

[4] WTO, Joint statement on Electronic Commerce, WT/MIN(17)/60, 13 December 2017.

[5] Ibid.

[6] The United States abandoned the Trans-Pacific Partnership (TPP) in January 2017 when President Donald Trump took office. The remaining eleven members, including Canada, signed the CPTPP in March 2018. The agreement entered into force on 30 December 2018, between Australia, Canada, Japan, Mexico, New Zealand and Singapore. The CPTPP entered into force in Vietnam on 14 January 2019. The agreement had yet to apply in Brunei, Chile, Malaysia and Peru at the time of writing.

[7] The USMCA was signed by all three parties on 30 November 2018, and ratified in Canada and Mexico in the spring of 2019, and by the United States in the beginning of 2020.

[8] The USMCA's chapter on digital trade builds on the CPTPP's electronic commerce chapter.

[9] Besides data-related issues, Ciuriak identifies a number of other important issues related to trade in digital goods and services that the WTO negotiations should address. See D. Ciuriak, 'World Trade Organization 2.0: Reforming Multilateral Trade Rules for the Digital Age', CIGI Policy Brief No 152 (2019).

[10] On 21 May 2019, the Government of Canada published its Digital Charter, which is a set of ten principles that are 'the building blocks of a foundation of trust for this digital age'; see www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html.

[11] Ibid.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

including on a cross-border basis', because data is 'intrinsic to commercial transactions'.[12] He sees data as the 'fifth freedom' of commerce, with free movement of goods, services, capital and labour as the other four. Legal and regulatory limits on cross-border data flows can, however, act as beyond-the-border obstacles to trade.[13] For instance, Martina Ferracane and Erik van der Marel find that policies that restrict the cross-border flow of data have a negative impact on trade in digital services.[14]

In certain circumstances (for example, to protect privacy, security, competition, culture, and so on), there is a need for the regulation of data collection, access, use and transfer. For example, the use of and access to people's data should be fair, transparent, accountable and subject to individuals' explicit consent. Moreover, the use of personal data should not lead to discrimination and bias when people seek to obtain a good or a service, whether it is from the private or the public sector. Another example is the protection of proprietary business data against uncompensated commercialization by others. On the other hand, access to data should not be controlled in such a way that it limits competition and innovation.

So the big question for policy-makers is how to allow for data to flow freely across borders while maintaining a high degree of trust among individuals, firms and governments that they will not be harmed in terms of privacy, consumption (price, choice or access), competition, innovation, security and so on. Strong data protection laws and regulations are necessary to create such trust. The problem is that such laws and regulations, if developed independently from other countries, can limit the cross-border flow of data and have negative economic consequences. This is the balancing act that the countries taking part in the WTO's plurilateral negotiations on 'trade-related aspects of electronic commerce' are trying to achieve.

C THE CPTPP, THE USMCA AND NATIONAL DATA REGULATION: EXAMPLE FROM CANADA

This section analyzes the electronic commerce/digital trade chapters included in the CPTPP and the USMCA in order to determine how they may affect data regulation in Canada, in order to provide an example of the potential impact that a WTO plurilateral agreement on trade-related aspects of electronic commerce modeled on CPTPP/USMCA provisions could have on members' governments'

[12] Ciuriak, note 9, at 6.

[13] Aaronson, note 1; D. Ciuriak and M. Ptashkina, *The Digital Transformation and the Transformation of International Trade* (Geneva/New York: ICTSD/IDB, 2018); N. Cory, 'Cross Border Data Flows: Where Are the Barriers, and What Do They Cost?', Information Technology and Innovation Foundation, May 2017; M. Rentzhog and H. Jonströmer, *No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden* (Stockholm: Kommerskollegium, 2014).

[14] M. F. Ferracane and E. van der Marel, 'Do Data Policy Restrictions Inhibit Trade in Services?', DTE Working Paper No 2 (2019); see also Chapter 3 in this volume.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

ability to regulate data nationally. Since the CPTPP's electronic commerce chapter provided the basis for the USMCA's digital trade chapter, the analysis focuses first on the CPTPP.[15]

I *The CPTPP*

The CPTPP contains several provisions in its chapter 14 (electronic commerce) that concern data flows.[16] Chapter 14 does not specify what types of data are covered, except to say those that are necessary for business purposes. It also preserves member states' ability to limit the free flow of data held by government entities and encourages interoperability between data privacy regimes as well as cooperation between consumer protection authorities.

Here are the CPTPP's main provisions relating to data flows:

- Consistent with the WTO's waiver on customs duties on electronic commerce, Article 14.3 prohibits the imposition of customs duties on electronic transmissions; however, it allows 'internal taxes, fees or other charges' as long as they are not discriminatory (i.e., applied equally to national as well as foreign entities).[17] As such, the CPTPP does not discriminate among various types or sources of data.
- Article 14.8 CPTPP mandates a personal data protection floor: it ensures that parties have laws and regulations that provide a minimum level of personal information protection but it is flexible as it accommodates different national approaches.[18]

[15] This section draws from P. Leblond, 'Digital Trade at the WTO: The CPTPP and CUSMA Pose Challenges to Canadian Data Regulation', CIGI Paper No 227 (2019).

[16] Consolidated TPP Text – chapter 14 – Electronic Commerce, Government of Canada, 30 November 2016, available at http://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng.

[17] Article 14.3 CPTPP, at para. 1: 'No Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of one Party and a person of another Party.

2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees or other charges on content transmitted electronically, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement'.

[18] Article 14.8 CPTPP, at paras. 2 and 3: 'To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.

Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction'.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

- Article 14.11 protects the free flow of cross-border data for business purposes,[19] although it allows restrictions on such flows in order to achieve a 'legitimate public policy objective'.[20]
- Article 14.13 prohibits the obligation for a business to locate specific computing facilities in exchange for market access.[21] In other words, it prohibits parties from imposing data localization requirements. However, the 'legitimate public policy objective' exception also applies in this case.
- Article 14.17 prohibits requirements that source code be transferred or accessed as a condition of import.[22] The prohibition is, however, limited to mass-market software but not when it is used in critical infrastructure.[23] The prohibition also does not apply to requests for source code modification to comply with domestic laws of regulations, as long as the latter are not inconsistent with the CPTPP; that is, they are not discriminatory in nature and apply equally to domestic and foreign firm.[24]

Article 14.2(3) CPTPP stipulates that 'this Chapter shall not apply to: (a) government procurement; or (b) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection'. This means that prohibitions on data transfer restrictions and data localization found in Articles 14.11 and 14.13 do not apply to governments. Therefore, the requirements imposed by the federal and some provincial governments that personal information held by public bodies be kept and processed in Canada are exempted under the CPTPP. This exception is potentially important if Canadian governments wish to make more publicly collected data available for analysis (for example, for artificial

[19] Article 14.11(2): 'Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person'.

[20] Article 14.11(3): 'Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective'.

[21] Article 14.13(2): 'No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'.

[22] Article 14.17(1): 'No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory'.

[23] Article 14.17(2): 'For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure'.

[24] Article 14.17(3)(b): 'Nothing in this Article shall preclude: a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement'.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

intelligence [AI] training purposes) but want to ensure that they retain control over them to protect individuals, as well as the state.

The scope of application of Article 14.2(3) CPTPP is, however, somewhat ambiguous, when it comes to subnational governments, especially part (b). This is because Article 1.3 defines 'Party' as 'any State or separate customs territory for which this Agreement is in force'. As such, it would exclude subnational governments at the provincial and municipal levels, especially since 'regional level of government' is defined separately in Article 1.3.[25] The term 'government procurement' in part (a) is less ambiguous. Article 15.2(2) CPTPP establishes the scope of application of government procurement: 'For the purposes of this Chapter, covered procurement means government procurement: (a) of a good, service or any combination thereof as specified in each Party's Schedule to Annex 15-A'. In Canada's schedule in Annex 15-A, section B deals with sub-central government entities.[26] Government procurement provisions do not apply to schools, universities, hospitals and Crown corporations for all provinces and territories except Ontario and Quebec.[27] This means that only in Ontario and Quebec (the excluded provinces) could such public entities impose localization restrictions with respect to data storage and processing in their procurement contract

Articles 14.11 and 14.13 CPTPP on the prohibition of, respectively, restrictions on cross-border data transfers for business purposes and requirements to localize the storage of data domestically, both contain an exception for a 'legitimate public policy objective'. This means that CPTPP parties, such as Canada, can restrict the in-and-out flow of data in order to pursue such an objective. The big question, however, is: what is a 'legitimate' objective? Article 14.11(3) states that a measure restricting cross-border data transfers cannot: (i) be 'applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised

[25] According to law professor Debra Steger, a state refers to a nation-state and does not cover subnational governments (separate customs territory refers to customs union, such as the European Union): 'No. A State is a nation state. A separate customs territory like the EU can also be a Party to a CU or an FTA under Art. XXIV GATT. University or hospital is a person or an enterprise', *Twitter*, 4 August 2018, available at https://twitter.com/DebraPS/status/1025643907097350144. This explanation was a reply to a tweet by the author: 'Calling on trade lawyers to tell me if the definition of "Party" in CPTPP Article 1.3 ("any State or separate customs territory") also covers subnational governments and their agencies or organizations (including hospitals and universities in the Canadian context). Thank you!', Twitter, 3 August 2018.

[26] Consolidated TPP Text – chapter 15-A – Government Procurement, Annex 15-A – Schedule of Canada, Government of Canada, 5 December 2016, available at http://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/15-a3.aspx?lang=eng.

[27] Ibid. Note 5 to section B in Canada's schedule in Annex 15-A says: 'For those provinces and territories marked by an obelisk (†), chapter 15 (Government Procurement) shall not cover the procurement of goods, services or construction services purchased for the benefit of, or which is to be transferred to the authority of, school boards or their functional equivalents, publicly-funded academic institutions, social services entities or hospitals'. Note 6 to section B applies to Crown corporations.

restriction on trade' and (ii) 'impose restrictions on transfers of information greater than are required to achieve the objective'. Article 14.13(3) offers the same limitation on the 'legitimate public policy objective' (also called general) exception:

> Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

Michael Geist questions whether privacy protection would qualify under the above-mentioned exception.[28] He seems doubtful when he writes: 'the [CPTPP] restriction on the use of data localization requirements may pose an insurmountable barrier'.[29] The same conclusion would apply to Article 14.11 CPTPP on data transfers. For instance, in early April 2019, the Office of the Privacy Commissioner of Canada (OPC) released a consultation paper on transborder data flows in which it indicates that it would require a company to obtain prior consent from individuals before moving their personal data outside of Canada.[30] According to Geist, this new approach 'is a significant reversal of longstanding policy that relied upon the accountability principle to ensure that organizations transferring personal information to third parties are ultimately responsible for safeguarding that information'.[31] The OPC stated that this new approach would be consistent with Canada's international trade obligations but Geist is not so sure: 'The imposition of consent requirements for cross-border data transfers could be regarded as imposing restrictions greater than required to achieve the objective of privacy protection, given that PIPEDA [Personal Information Protection and Electronic Documents Act] has long been said to provide such protections through accountability without the need for this additional consent regime'.[32]

Andrew Mitchell and Neha Mishra, for their part, also point out that there is the potential for conflict between e-commerce or digital trade chapters in free trade

[28] M. Geist, 'Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards', in CIGI (ed), *Special Report: Data Governance in the Digital Age* (Waterloo: CIGI, 2018).

[29] Ibid.

[30] Office of the Privacy Commissioner of Canada, 'Consultation on Transborder Dataflows', 11 June 2019, available at www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/.

[31] Geist, note 28. In light of the government's publication of the Digital Charter, the OPC reframed its consultation in June 2019, putting less emphasis on its interest in requiring businesses to obtain prior consent from individuals before transferring their data abroad. See Office of the Privacy Commissioner of Canada, 'Consultation on Transfers for Processing – Reframed Discussion Document', 11 June 2019, available at www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/.

[32] There are two federal laws that govern personal data and information in Canada. The Privacy Act sets the rules for how the federal public sector collects, uses and discloses personal information. The Personal Information Protection and Electronic Documents Act (PIPEDA)

agreements (FTAs) and WTO agreements, such as the General Agreement on Trade in Services (GATS).[33] They write that Article XIV GATS provides the basis for the general exception found in FTA provisions, such as the CPTPP's Articles 14.11 and 14.13; however, they also note that 'these exceptions may be unable to address all aspects of data flow restrictions'.[34] In addition, Mitchell and Mishra mention that 'strict scrutiny of these measures [restricting data flows] under international trade law may lead to unsatisfactory outcomes because GATS Articles XIV and XIV *bis* are limited in scope and do not facilitate consideration of Internet trust issues holistically'.[35] The above implies that general exceptions on data transfers and data localization found in the CPTPP may not offer as much policy flexibility as originally thought with respect to future laws and regulations that Canadian (federal and provincial) governments might want to put into place to govern data in order to ensure trust as well as stimulate innovation.

Given that algorithms 'drive what news content and advertising each of us sees online [and] will be used by governments to decide who receives or is denied benefits',[36] it is reassuring that Article 14.17 CPTPP does not prevent governments from regulating and supervising source codes, as long as it is not done in a protectionist way against foreign producers. Teresa Scassa notes that it is necessary to be able to access the source code of an app, software or AI in order to evaluate algorithms' performance and potential biases.[37] Such enquiries are important if governments want to protect consumers, workers and businesses from suffering the negative consequences associated with, for example, fraud or discrimination.

does the same for the private sector. See Office of the Privacy Commissioner of Canada, 'Summary of Privacy Laws in Canada', 31 January 2018, available at www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/. PIPEDA only applies to commercial, for-profit activities. As such, it does not apply to non-profit and charity organizations, unless they conduct commercial activities that involve personal information. The OPC, which is responsible for implementing both acts, defines personal information as 'data about an identifiable individual [. . .] that on its own or combined with other pieces of data, can identify you as an individual'. See Office of the Privacy Commissioner of Canada, 'The Digital Privacy Act and PIPEDA', November 2015. As such, it indicates that the following types of information are not (generally) considered personal: information about a business or an organization; information that is not possible to link back to an identifiable person (i.e., it has been anonimized); and information that is not about an individual and whose connection with a person is too weak or far-removed.

[33] A. D. Mitchell and N. Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy', *Vanderbilt Journal of Entertainment and Technology Law* 20 (2018), 1073–1134.

[34] Ibid., at 1095.

[35] Ibid.; also Creach, who writes that 'given the stringent conditions for trade restrictions to fall within the scope of GATS Article XIV (especially the necessity test), one may doubt that data-localization requirements are justifiable'. See M. Creach, 'Assessing the Legality of Data-Localization Requirements: Before the Tribunals or at the Negotiating Table?', Columbia FDI Perspectives No 254 (2019), at 2.

[36] T. Scassa, 'What Role for Trade Deals in an Era of Digital Transformation?', *CIGI*, 4 October 2018, available at www.cigionline.org/articles/what-role-trade-deals-era-digital-transformation.

[37] Ibid.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

II *The USMCA*

The USMCA, unlike NAFTA, which it replaces, contains a chapter (19) on 'digital trade' (not 'e-commerce', in order to signify its broader scope) that builds on the CPTPP's chapter 14.[38] As such, the USMCA introduces a number of differences from the CPTPP. The following analysis focuses on these differences.

One significant difference with the CPTPP concerns the requirement for USMCA member states to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade'.[39] While the USMCA does not prescribe specific rules or measures that a party must take to protect privacy, it goes further than the CPTPP by providing more guidance to inform a country's privacy regime. In particular, the USMCA refers explicitly to the APEC (Asia-Pacific Economic Cooperation) Privacy Framework and OECD (Organisation for Economic Co-operation and Development) Guidelines as relevant 'principles and guidelines' when developing a legal framework for protecting personal information.[40] Unlike the CPTPP, the USMCA also mentions key principles that parties should follow as they develop their legal framework.[41]

In addition, the USMCA stipulates that the parties 'recognize the importance of . . . ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented',[42] thereby providing some limit on the extent to which data protection legislation or regulation can constrain cross-border personal data flows. Such a standard for potentially restricting data flows in order to protect personal information is not present in the CPTPP's Article 14.8(2). As such, the USMCA provides some guidance, albeit vague, to future panel arbitrators in interpreting the 'legitimate public policy objective' exception in the case of a dispute involving limits imposed on cross-border data flows by one of the USMCA parties. The big issue in this case is what 'necessary and proportionate' mean in the context of protecting personal information? For instance, would a requirement for organizations in Canada to obtain explicit consent from individuals before the latter's data are transferred across the border to the United States be deemed necessary and proportionate?

[38] Government of Canada, Canada–United States–Mexico Agreement (CUSMA) – Table of Contents, 21 February 2020, available at www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/toc-tdm.aspx?lang=eng.

[39] Article 19.8(2) USMCA.

[40] The CPTPP's Article 14.8(3) states only that 'each Party should take into account principles and guidelines of relevant international bodies' (it does not mention any particular international body, however).

[41] The USMCA's Article 19.8(3) states: 'The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability'.

[42] Article 19.8(3) USMCA.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

What is probably the most important difference between the USMCA and the CPTPP is the former's Article 19.17 on Interactive Computer Services, which has no equivalent in the CPTPP. According to this article, Internet service providers, social media platforms and search engines cannot be treated as information content providers for liability purposes, which means 'immunity from legal consequences for content generated by users'.[43] However, Annex 19-A(4) states: 'For greater certainty, Article 19.17 (Interactive Computer Services) is subject to Article 32.1 (General Exceptions), which, among other things, provides that, for purposes of chapter 19, the exception for measures necessary to protect public morals pursuant to paragraph (a) of Article XIV of the GATS is incorporated into and made part of this Agreement, *mutatis mutandis*'. This paragraph opens the door for potential limits on the article's scope and application but, as mentioned earlier, there is a lot of uncertainty with respect to the general exception's reach.[44] In any case, the USMCA's Article 19.17 will likely make it harder for Canadian governments to develop measures to protect individuals and consumers of social media, search engines and other user-generated content providers from the consequences of disinformation (for example, 'fake news').

Another noteworthy difference between the USMCA and the CPTPP concerns source code and algorithms. First, the USMCA's Article 19.16 gets rid of the CPTPP's Article 14.17(2).[45] This implies that all types of source code are covered by the USMCA, without exception. As Scassa notes: 'This may raise some interesting concerns given the growing government use of software and algorithms in key systems and processes'.[46] The USMCA also does not contain the CPTPP's provision on allowing requests for source code modification.[47] Instead, it offers Article 19.16(2), which does not exist in the CPTPP: 'This Article does not preclude a regulatory

[43] T. Israel and L. Tribe, 'Did NAFTA 2.0 Sign Away Our Digital Future?', *Ottawa Citizen*, 15 October 2018. The USMCA's Article 19.17(3) states: 'No Party shall impose liability on a supplier or user of an interactive computer service on account of: (a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or (b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable'.

[44] This is why Nancy Pelosi, Speaker of the US House of Representatives, pushed, unsuccessfully, to have this provision removed at the last minute to secure the USMCA's congressional approval because she and other members of Congress were concerned that the USMCA's Article 19.17 could 'damage domestic efforts to amend the Section 230 law'. The USMCA's provision is based on Section 230 of the US Communications Decency Act.

[45] The CPTPP's Article 14.17(2) states: 'For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure'.

[46] Scassa, note 36.

[47] The CPTPP's Article 14.17(3)(b) states: 'Nothing in this Article shall preclude a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement'.

body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure'. Scassa says that the difference between the USMCA and the CPTPP provisions is 'important given that we are already facing context in which it is necessary to understand the algorithms that lead to certain decisions [for example, litigation involving autonomous vehicles]'.[48] So the USMCA improves on the CPTPP in terms of source code transparency but it is also a step back when it comes to the absence of a provision allowing requests to modify algorithms, which could be found to be biased or causing harm to people, businesses or governments. With the USMCA, unlike the CPTPP, a Canadian request for algorithmic modification could be challenged as a protectionist measure discriminating against the US or Mexican producer of the software or application.

The final difference between the USMCA and the CPTPP is with respect to the provisions on data localization ('Location of Computing Facilities'). In the CPTPP's Article 14.13, 'the Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications'[49] but 'no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'[50] unless it is for a 'legitimate public policy objective'.[51] For its part, the USMCA's Article 19.12 only has one provision: 'No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.' This means that, unlike the CPTPP, the USMCA does not allow its parties to invoke a 'legitimate public policy objective' exception to impose a data localization requirement to firms from the other two parties as a condition for providing a digital good or service in the territory. The only exception possible here is for the specific case when a digital good or service is provided to a government, because the USMCA's chapter 19 does not apply to 'government procurement; or except for Article 19.18 (Open Government Data), to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection'.[52] Therefore, governments can only require

[48] Scassa, note 36.
[49] Article 14.13(1) CPTPP.
[50] Article 14.13(2) CPTPP.
[51] Article 14.13(3) CPTPP. The CPTPP's Article 14.13(3) states: 'Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective'.
[52] Article 19.2(3).

organizations that collect, hold or process information to locate their computing facilities in the territory when these activities are undertaken for or on behalf of a government, which is in line with current practices. However, if, for example, data deemed critical for national security reasons were held by a private organization, then the USMCA would technically require a government to allow these data to be held and processed in the other two member states' territory. As a result, these data could become accessible to the other member state governments (for example, through the USA PATRIOT Act in the United States).

III *Interim Conclusion*

With the CPTPP and the USMCA, Canada has adopted obligations that provide for the free flow across borders of data for business purposes while, in principle, protecting consumers, personal information and government-related data. However, as analyzed earlier, these two trade agreements also pose potential obstacles to Canada's ability to effectively regulate data and it is unclear how much policy flexibility they leave to the federal and provincial governments to pursue legitimate objectives and protect the vital interests of their citizens. It will ultimately be left to state-to-state dispute settlement panels in the CPTPP and the USMCA (as well as the investor–state dispute settlement mechanism in the CPTPP) to resolve this uncertainty and determine the scope of Canada's national data regulation. If dispute settlement panels were to rule in favour of cross-border data flows and impose limits on Canada's ability to ensure trust among individuals and businesses when it comes to the data-driven economy, then such decisions could undermine the CPTPP's and the USMCA's legitimacy and political support.

D KEY PROPOSALS AT THE WTO'S PLURILATERAL NEGOTIATIONS ON TRADE-RELATED ASPECTS OF ELECTRONIC COMMERCE

In April 2019, the key players in the negotiations – China, the EU and the United States – issued their proposals to the WTO's plurilateral negotiations on trade-related aspects of electronic commerce.[53] The Chinese proposal is the least ambitious. It is hortatory in nature and focuses on principles for the facilitation of cross-border electronic commerce, leaving aside data flows.[54] China's proposal is thus in

[53] For China's proposal, see WTO, Joint Statement on Electronic Commerce, Communication from China, INF/ECOM/19, 24 April 2019. For the European Union's proposal, see WTO, Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22, 26 April 2019 [hereinafter: EU Proposal]. For the US proposal, see WTO, Joint Statement on Electronic Commerce, Communication from the United States, INF/ECOM/23, 26 April 2019 [hereinafter: US Proposal].

[54] Specifically, Article 4.2 of China's proposal states that issues such as data flows and data storage require 'more exploratory discussions … before bringing [them] to the WTO negotiation'. In

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

line with the electronic commerce provisions contained in some of the FTAs that it has signed so far. As such, it reflects the country's desire to protect its walled-off digital realm.[55]

The EU's proposal goes much further than the Chinese one. For instance, it offers specific provisions that mandate unrestricted cross-border data flows,[56] subject to national rules deemed 'appropriate to ensure the protection of personal data and privacy'.[57] The EU's proposal also stipulates that there can be no requirement for the transfer of software source codes in exchange for market access, although it can be required for legal violations or national security reasons.[58]

The US proposal, for its part, follows closely the digital trade chapter found in the USMCA.[59] As such, it supports the EU's position on cross-border data flows, personal data protection and source codes; however, unlike the EU's proposal, which states that '[n]othing in the agreed disciplines and commitments shall affect the protection of personal data and privacy afforded by the Members' respective safeguards',[60] the US offer qualifies the limits on cross-border data flows that national data protection regimes can impose: 'ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented' (Article 7.4), which follows USMCA's Article 19.8.3. Article 8 of the US proposal also restates, verbatim, the USMCA's provision[61] that only restrictions on cross-border data flows that 'achieve a legitimate public policy objective' are acceptable. Finally, the USMCA's Article 19.17 ('Interactive Computer Services') is transposed in its entirety into the US proposal,[62] thereby putting forward the prohibition on treating 'a supplier or user of an interactive computer services as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent that the supplier or user has, in whole or in part, created or developed the information'.[63]

Article 4.3, the proposal adds, 'the data flow [sic] should be subject to the precondition of security, which concerns each and every Members' core interests. To this end, it is necessary that the data flow orderly [sic] in compliance with Members' respective laws and regulations'.

55 S. A. Aaronson and P. Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO', *Journal of International Economic Law* 21 (2018), 245–272. See also Chapter 12 in this volume.

56 EU Proposal, note 53, section 2.7.

57 Ibid., section 2.8.

58 Ibid., section 2.6.

59 B. Baschuk, 'US WTO E-Commerce Offer Reflects USMCA Digital Trade Chapter', *Bloomberg Law*, 6 May 2019; I. Manak, 'US WTO E-Commerce Proposal Reads Like USMCA', *International Economic Law and Policy Blog*, 8 May 2019, available at https://worldtradelaw.typepad.com/ielpblog/2019/05/us-wto-e-commerce-proposal-reads-like-usmca.html.

60 EU Proposal, note 53, section 2.8 EU.

61 Article 19.11 USMCA.

62 US Proposal, note 53, Article 13.

63 US Proposal, note 53, Article 13.2.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

FIGURE 14.1. Illustrating the relative positions of the main proposals to the WTO's plurilateral negotiations on e-commerce

In sum, the proposals occupy different places on a continuum that includes independent national data protection at one end and cross-border data free flow at the other, with China being close to the former pole while the United States is closer to the other pole and the EU is somewhere in between (see Figure 14.1). As analyzed earlier, the USMCA's digital trade chapter, which itself builds on the CPTPP's chapter 14, has served to inform the US position in the WTO's Plurilateral 'Trade-related Aspects of Electronic Commerce' negotiations. Should the latter ever prevail, which remains to be seen in light of the divergent key positions on offer, it will make it difficult for member states to adopt national data regulations that impose limits on the cross-border flow of data, most especially personal data.

E CONCLUSION AND OUTLOOK

As the example of Canada demonstrates herein, the CPTPP and the USMCA require their members to adopt obligations that provide for the free flow across borders of data for business purposes while, in principle, protecting consumers, personal information and government-related data. However, as analyzed above, these two trade agreements also pose potential obstacles to a member state's ability to effectively regulate data and provide a trustworthy environment for individuals, businesses and governments. The analysis shows that it is not at all clear how much policy flexibility the CPTPP and the USMCA ultimately allow governments that want to adopt new laws and regulations to, among various objectives, protect people's privacy, prevent algorithmic bias, protect critical infrastructure, ensure national security or promote domestic innovation.

For the plurilateral negotiations of an agreement on 'trade-related aspects of electronic commerce' at the WTO, this means that the US proposal, which is closely derived from the USMCA's digital trade chapter,[64] would create a lot of uncertainty as to how much limits on cross-border data flows a country could impose via its national data regulation regime, until dispute-settlement panels decide on the acceptability and legitimacy of national data rules in restricting data flows across borders.

[64] Chapter 19 USMCA.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press

To leave such crucial decisions for economy and society in the hands of unelected and unaccountable individuals seems an odd way to govern the data-driven economy's future functioning. A better approach would be to remove issues related to data regulation and standards from the WTO negotiations and push for a separate international regime to govern data and its cross-border flows.[65] Just like capital (or financial) flows are not part of the WTO's framework,[66] which limits itself to rules on trade in financial services, so should data flows be excluded from an eventual agreement on trade-related aspects of electronic commerce. The latter agreement, should it ever see the light of day, should instead focus its attention solely on the rules governing trade in digital goods and services. A separate international body (such as an International Data Standards Board) should be responsible for setting standards that regulate the creation, processing, use, distribution and transfer of data, both personal and non-personal. All countries that apply and enforce these standards would be allowed to take part in a single data area where data would be free to flow across member states' borders. The WTO's rules on digital trade would be left to deal with possible infringement of core trade principles, such as non-discrimination.

[65] P. Leblond and S. A. Aaronson, 'A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma', CIGI Papers No 226 (2019).

[66] The Financial Stability Board oversees and coordinates the various international bodies that set the standards that govern finance.

https://doi.org/10.1017/9781108919234.019 Published online by Cambridge University Press